

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DANIEL FRASER,

Plaintiff,

v.

MINT MOBILE, LLC,

Defendant.

No. C 22-00138 WHA

**ORDER RE MOTION TO DISMISS**

---

**INTRODUCTION**

Hackers took cell phone users' information from their carrier and this information was used to port plaintiff's cellular service to another carrier whereupon a criminal pretending to be plaintiff acquired access to and then drained plaintiff's cryptocurrency account maintained by a cryptocurrency exchange. The issue is the extent to which the carrier is liable for the lost funds once held by the cryptocurrency exchange. For the following reasons, the motion to dismiss is **GRANTED IN PART** and **DENIED IN PART**.

**STATEMENT**

Defendant Mint Mobile, LLC is a mobile virtual network operator that currently uses T-Mobile's network infrastructure to provide wireless cellular services to its customers. One of those customers was plaintiff Daniel Fraser. This action involves three incidents that

1 eventually led to the theft of Fraser’s cryptocurrency, held by a non-party cryptocurrency  
2 exchange.

3 *First*, between June 8, 2021, and June 10, 2021, Mint (the mobile carrier) suffered a  
4 large-scale data breach. The leak exposed the personal identifying information (PII) of many  
5 of its cellphone customers, including their names, addresses, email addresses, phone numbers,  
6 account numbers, and passwords. Fraser was one of the customers affected by the breach  
7 (Compl. ¶¶ 3, 12).

8 *Second*, criminals purportedly used the information exposed in the data breach to hijack  
9 Fraser’s cellphone service. SIM hijacking represents a growing crime in telecommunications.  
10 A subscriber identity module, or “SIM” card, authenticates a cellphone subscription. Switch  
11 the SIM card from an old phone into a new phone and the cellular service shifts to the new  
12 device.

13 Relevant here, SIM porting, or port-out fraud, is a genus of SIM hijacking where a  
14 criminal, posing as the victim, opens an account with a carrier different from that of the hacked  
15 carrier and arranges for the victim’s cellular service to be transferred to the new carrier and put  
16 under control of the criminal. On June 11, 2021, an unknown criminal ported Fraser’s cellular  
17 service with Mint to another service provider, Metro by T-Mobile. Fraser alleges that the  
18 earlier Mint data breach exposed all the information needed to port out his service.

19 Additionally, Fraser alleges that, three days before his service was fraudulently ported to the  
20 other provider, he had implemented a PIN verification feature on his Mint account to enhance  
21 his electronic security with two-factor authentication, *i.e.*, making changes to his account  
22 required both a password and a pin verification code. Fraser alleges that Mint bypassed this  
23 enhanced security when it allowed the porting out of his account. All of this occurred before  
24 Mint notified affected customers of the breach on July 9, 2021 (Compl. ¶¶ 2–6, 37–43, 59–66).

25 *Third*, Fraser’s cryptocurrency account (with a completely separate firm) was then  
26 hacked and his assets stolen. Besides the loss of one’s cell service, port-out fraud places the  
27 victim’s other personal accounts at risk as well. Personal accounts — *e.g.*, for email, banking,  
28 or cryptocurrency — will often use the account holder’s telephone number as a means for the

1 account holder to recover access to their account when, for example, they forget their  
2 password. In many instances, all the account holder needs to do to regain access to their  
3 account is verify their identity by entering a pin number automatically sent to their phone via  
4 their cellular service (like the pin verification Fraser put on his Mint account). This means  
5 once a criminal successfully ports a victim's cellphone service, the criminal acquires a key to  
6 steal the victim's identity and access a variety of the victim's accounts (so long as the criminal  
7 has other, basic information regarding the victim's accounts, such as the email address used to  
8 maintain the account) (Compl. ¶¶ 1, 49, 59 62–67).

9 Fraser had an account with Ledger, a specific cryptocurrency exchange, where he stored  
10 his cryptocurrency. He alleges that the combination of Mint's data breach (which occurred  
11 from June 8 through June 10) and the fraudulent SIM port (which occurred on June 11 at 8:08  
12 a.m.) provided criminals with all the information and access required to hack into and drain his  
13 Ledger account (Compl. ¶ 63). As a result, starting on June 11 at 9:19 a.m., a criminal began  
14 to drain Fraser's Ledger account, and eventually stole the equivalent of \$466,000.00 in  
15 cryptocurrency (Compl. ¶¶ 59–67).

16 Fraser filed this lawsuit to hold Mint responsible for its purported role in the theft of his  
17 cryptocurrency. Fraser broadly asserts claims for violation of the Federal Communications  
18 Act, violations of California Business & Professions Code Section 17200, negligence, and  
19 breach of contract. He does not assert his claims on behalf of a putative class. Now, Mint  
20 moves to dismiss the complaint for failure to state a claim. At the hearing, Mint withdrew its  
21 motion to dismiss the prayer for injunctive relief pursuant to the Federal Communications Act  
22 as well as its motion to compel arbitration. This order follows full briefing and oral argument.

### 23 ANALYSIS

24 A motion to dismiss tests the legal sufficiency of the complaint. To survive a motion to  
25 dismiss under Rule 12(b)(6), a complaint must contain sufficient factual matter, accepted as  
26 true, to state a claim for relief that is plausible on its face. A claim is facially plausible when  
27 there are sufficient factual allegations to draw a reasonable inference that the defendant is  
28 liable for the misconduct alleged. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). While a court

1 must take all of the factual allegations in the complaint as true, it is “not bound to accept as  
2 true a legal conclusion couched as a factual allegation.” *Bell Atl. Corp. v. Twombly*, 550 U.S.  
3 544, 555 (2007). “Factual allegations must be enough to raise a right to relief above the  
4 speculative level.” *Ibid*.

5 **1. PROXIMATE CAUSE (ALL COUNTS).**

6 Mint argues that the complaint fails to adequately allege the data breach and SIM port  
7 proximately caused the theft of Fraser’s cryptocurrency from a third-party, and that the  
8 complaint should be dismissed in its entirety (Br. 6). This order disagrees.

9 “It is a well established principle of the common law that in all cases of loss, we are to  
10 attribute it to the proximate cause, and not to any remote cause.” *Bank of Am. Corp. v. City of*  
11 *Miami*, 137 S. Ct. 1296, 1305 (2017) (cleaned up). Generally, the proximate cause  
12 requirement “bars suits for alleged harm that is ‘too remote’ from the defendant’s unlawful  
13 conduct.” *Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 133 (2014).  
14 Under California law, proximate cause has two aspects. The *first* is cause in fact, sometimes  
15 referred to as but-for causation. Under the substantial factor test, which generally subsumes  
16 but-for causation, a cause in fact is an act or omission that was a substantial factor in bringing  
17 about the plaintiff’s harm. The *second* aspect of proximate cause incorporates considerations  
18 of public policy. “These additional limitations are related not only to the degree of connection  
19 between the conduct and the injury, but also with public policy.” *State Dep’t of State Hosps. v.*  
20 *Super. Ct.*, 61 Cal. 4th 339, 352–53 (2015) (quotation omitted); *Frausto v. Dep’t of Cal.*  
21 *Highway Patrol*, 53 Cal. App. 5th 973, 996 (2020). “Ordinarily, proximate cause is a question  
22 of fact which cannot be decided as a matter of law from the allegations of a complaint.  
23 Nevertheless, where the facts are such that the only reasonable conclusion is an absence of  
24 causation, the question is one of law, not of fact.” *State Hosps.*, 61 Cal. 4th at 353 (cleaned  
25 up).

26 *First*, Mint argues that “holes in [p]laintiff’s conclusory chain of causation overcome  
27 proximate causation” (Br. 8). The complaint, however, adequately explains how the  
28 combination of Mint’s data breach and the SIM port-out gave criminals the information and

1 access needed to drain Fraser’s Ledger account. The data breach exposed, among other  
 2 information, Fraser’s name, address, telephone number, email address, and Mint password.  
 3 Moreover, the data breach did not merely expose some of Fraser’s PII, it purportedly revealed  
 4 the specific PII necessary for a criminal to port out Fraser’s wireless service to an account  
 5 under the criminal’s control (Compl. ¶¶ 61–63).

6 Mint argues the complaint does not adequately connect the dots between its conduct and  
 7 the theft of Fraser’s cryptocurrency from his Ledger account. Fraser alleges, however, that  
 8 once a criminal gains access to a victim’s email, it is a straight-forward inquiry to determine  
 9 what sort of financial accounts the victim maintains. A simple query of the victim’s email  
 10 account would reveal any number of accounts a criminal could then try to access (*id.* ¶¶ 59–  
 11 67). That logical progression suffices. Remember, the criminal began draining Fraser’s  
 12 Ledger account at 9:19 a.m., just one hour, eleven minutes after the SIM port-out. And the  
 13 SIM port-out occurred (at most) a few days after the Mint data breach. The allegations of  
 14 proximate cause here are sufficiently direct and not comparable to the “Rube Goldbergesque  
 15 system of fortuitous linkages” where California courts have held proximate cause lacking as a  
 16 matter of law. *Steinle v. United States*, 17 F.4th 819, 822–23 (9th Cir. 2021).

17 *Second*, Mint contends the allegations fail due to their reliance upon multiple  
 18 independent illegal acts of third parties (Br. 9). Under California law: “The defense of  
 19 superseding cause absolves the original tortfeasor, even though his conduct *was* a substantial  
 20 contributing factor, when an independent event subsequently intervenes in the chain of  
 21 causation, producing harm of a kind and degree so far beyond the risk the original tortfeasor  
 22 should have foreseen that the law deems it unfair to hold him responsible.” *Chanda v. Fed.*  
 23 *Home Loans Corp.*, 215 Cal. App. 4th 746, 755 (2013) (cleaned up). In other words:

24 To qualify as a superseding cause so as to relieve the defendant  
 25 from liability for the plaintiff’s injuries, both the intervening act  
 26 and the results of that act must not be foreseeable. . . . Whether an  
 27 intervening force is superseding or not generally presents a  
 28 question of fact, but becomes a matter of law where only one  
 reasonable conclusion may be reached.

1 *Id.* at 755–56. Here, “it could hardly be argued that the risk of the harm that befell plaintiffs  
2 was as a matter of law unforeseeable.” *Lawson v. Safeway Inc.*, 191 Cal. App. 4th 400, 417  
3 (2010). Fraser alleges that Mint provided criminals with all the information and access they  
4 needed to hack his accounts and steal his assets (Compl. ¶ 63). He further explains that SIM  
5 hijacking represents a national problem, one that has spurred FCC action (Compl. ¶¶ 68–80).  
6 At this posture, given the known threat of SIM hijacking and that Mint purportedly bypassed  
7 the pin verification Fraser set up, the complaint plausibly alleges foreseeable acts that do not  
8 qualify as superseding causes.

9 Mint disagrees and asserts it “lacks the legal and practical ability to control the acts of  
10 criminals” (Br. 10). “However, this expectation does not exonerate a defendant whose  
11 ‘conduct has created or increased the risk of harm.’” *Lawson*, 191 Cal. App. 4th at 418  
12 (quoting Rest. 2d Torts § 449, cmt. a). The modern standard addressed herein does not take  
13 the rigid view Mint proposes that criminal acts necessarily constitute superseding causes. *See*  
14 *also Bigbee v. Pac. Tel. & Tel. Co.*, 34 Cal. 3d 49, 58 (1983); 6 Witkin, Summary of Cal. Law,  
15 Torts § 1366 (11th ed. 2021). The opinions that Mint cites are inapposite. For example, the  
16 decision in *Martinez v. Pacific Bell*, 225 Cal. App. 3d 1557, 1565–66 (1990), is distinguishable  
17 because, in that matter, plaintiff asserted a telephone company proximately caused his injuries  
18 resulting from a robbery because the robbers were attracted to the neighborhood because of a  
19 public telephone booth. In contrast, Mint’s conduct here much more directly created or  
20 increased the risk of harm. Other cited cases do not address California law or apply the  
21 previous standard. *See Citizens Bank of Pa. v. Reimbursement Techs., Inc.*, 2014 WL 2738220,  
22 at \*3 (E.D. Pa. June 17, 2014) (Judge L. Felipe Restrepo); *O’Keefe v. Inca Floats, Inc.*, 1997  
23 WL 703784, at \*4 (N.D. Cal. Oct. 31, 1997) (Judge Vaughn R. Walker); *Jesse v. Malcmacher*,  
24 2016 WL 9450683, at \*10 (C.D. Cal. Apr. 5, 2016) (Judge Stephen V. Wilson). Fraser  
25 plausibly alleges that Mint’s data breach and role in the SIM port-out created the opportunity  
26 for the cryptocurrency theft.

27 In sum, at least at this stage, where pleadings are liberally construed and the pleader has  
28 not yet had an opportunity to obtain discovery, this order holds it was reasonably foreseeable to

both plaintiff and defendant that a breach of the type alleged of defendant's system would pose the risk of a follow-on injury of the type alleged.

## 2. SECTION 17200 CLAIMS. (COUNTS IV–VI).

Turning to Fraser's Section 17200 claims, Mint argues that Fraser cannot be awarded monetary damages pursuant to Section 17200 and that he has not adequately pleaded he is entitled to restitution (Br. 10–11).

*First*, California's unfair competition law prohibits any "unlawful, unfair or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200 *et seq.* Although a plaintiff must allege a loss of money or property caused by the purported unfair competition to qualify for relief, the remedies available under a Section 17200 claim are limited to restitution and injunctive relief. *Id.* § 17204; *Clark v. Super. Ct.*, 50 Cal. 4th 605, 610 (2010). This order consequently **DISMISSES WITH PREJUDICE** the remedies sought in the "Wherefore" paragraphs contained within Counts IV–VI to the extent they seek relief beyond restitution and injunctive relief for violations of Section 17200.

*Second*, the complaint fails to adequately state a claim for restitution. In the context of Section 17200, "restitution means the return of money to those persons from whom it was taken or who had an ownership interest in it." *Shersher v. Super. Ct.*, 154 Cal. App. 4th 1491, 1497 (2007) (citation and quotation omitted); *see also Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1149 (2003).

Here, Fraser vaguely alleges in Count IV that "Plaintiff has lost the benefit of his bargain for his purchased services from Mint that he would not have paid had he known the truth regarding Mint's inadequate data security" (Compl. ¶ 166). His Section 17200 allegations focus, however, on how the "harm caused by Mint's actions and omissions . . . is substantial in that it has caused Plaintiff to suffer approximately \$466,000.00 in actual financial harm because of Mint's unfair business practices (*id.* ¶ 186; *see also* ¶¶ 165, 194). But a "restitution order against a defendant thus requires both that money or property have been lost by a plaintiff, on the one hand, and that it have been acquired by a defendant, on the other." *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310, 336 (2011). It was not Mint that acquired



Fraser’s cryptocurrency, but a third-party criminal. Fraser, consequently, has failed to allege he is entitled to restitution from Mint. Because Fraser does not seek injunctive relief, he fails to adequately state a claim for relief under Section 17200, generally. Counts IV, V, and XI are accordingly **DISMISSED**.

### 3. COMPUTER FRAUD AND ABUSE ACT (COUNT III).

Next up is Fraser’s Computer Fraud and Abuse Act (CFAA) claim. Mint contends this claim should be dismissed because the complaint fails to adequately plead conduct and losses necessary for a civil CFAA claim.

“The CFAA was enacted in 1984 to enhance the government’s ability to prosecute computer crimes.” *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130 (9th Cir. 2009). The CFAA also includes a private right of action. 18 U.S.C. § 1030(g). To state a civil claim under the CFAA, the plaintiff must allege: (1) that he or she “suffer[ed] damage or loss by reason of [the defendant’s] violation” of the Act; and (2) that one of five enumerated circumstances in Section 1030(c)(4)(A)(i)(I) through (V) is present.

Fraser generally alleges Mint violated CFAA Sections 1030(a)(2)(C) and 1030(a)(4). Section 1030(a)(2)(C) ascribes liability to one who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer.” Section 1030(a)(4), in turn, finds liable one who “knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period.” Fraser then further alleges, per Section 1030(c)(4)(A)(i)(I), losses aggregating more than \$5,000 in value (Compl. ¶¶ 146, 151).

As an initial matter, Fraser has asserted an aiding and abetting theory of liability (Compl. ¶ 146). As Judge Beth Labson Freeman of our district recently explained in *Nowak v. Xapo, Inc.*, 2020 WL 6822888, at \*4 (N.D. Cal. Nov. 20, 2020), it is an open question whether such a claim can be asserted under the CFAA in a civil suit. Regardless, the parties failed to brief



1 aiding-and-abetting liability and this order finds Fraser’s CFAA claim fails for the more  
2 fundamental reason that the pleading does not adequately allege harm recognized under the  
3 Act.

4 The CFAA defines “damage” as “any impairment to the integrity or availability of data, a  
5 program, a system, or information.” 18 U.S.C. § 1030(e)(8). It defines “loss” as “any  
6 reasonable cost to any victim, including the cost of responding to an offense, conducting a  
7 damage assessment, and restoring the data, program, system, or information to its condition  
8 prior to the offense, and any revenue lost, cost incurred, or other consequential damages  
9 incurred because of interruption of service.” *Id.* § 1030(e)(11). As the Supreme Court recently  
10 held: “The statutory definitions of ‘damage’ and ‘loss’ thus focus on technological harms —  
11 such as the corruption of files — of the type unauthorized users cause to computer systems and  
12 data. . . . The term’s definitions are ill fitted, however, to remediating ‘misuse’ of sensitive  
13 information. . . .” *Van Buren v. United States*, 141 S. Ct. 1648, 1659–60 (2021). In other  
14 words, “the CFAA creates the right to recover damages and losses related to a computer or  
15 system, not damages that flow from the use of unlawfully obtained information.” *Delacruz v.*  
16 *State Bar of Cal.*, 2017 WL 7310715, at \*6 (June 21, 2017) (Judge Susan Van Keulen), *report*  
17 *and recommendation adopted*, 2017 WL 3129207 (N.D. Cal. July 24, 2017) (Judge Beth  
18 Labson Freeman).

19 Here, the complaint recites only conclusory allegations that, due to Mint’s conduct and  
20 the interruption of “[p]laintiff’s service, he has suffered damage far in excess of Five Thousand  
21 Dollars” (Compl. ¶¶ 151–52). The only damage or loss that Fraser cites in his complaint,  
22 however, is the theft of his cryptocurrency, which does not constitute loss related to a computer  
23 or system. Rather, the loss here flows from the use of the unlawfully obtained information to  
24 hack Fraser’s Ledger account. This order finds this type of damage or loss is not recognized  
25 by the CFAA. *See also Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1263 (9th Cir. 2019).

26 Accordingly, the CFAA claim is **DISMISSED**.

#### 27 **4. CONTRACT-RELATED CLAIMS (COUNT XI, XII).**

28 Mint next challenges two of Fraser’s contract-related claims.

1           First, Mint argues that the claim for breach of the implied covenant of good faith and fair  
2 dealing should be dismissed because Fraser merely alleges that Mint failed to comply with the  
3 express terms of the contract (Br. 23). This order finds the implied covenant claim duplicative  
4 of Fraser’s breach of contract claim. The only justification for asserting a separate cause of  
5 action for breach of the implied covenant is to obtain a tort recovery in those limited  
6 circumstances in which such tort recovery is allowed. Those narrow circumstances do not  
7 apply here. *See Nasser v. Wells Fargo Bank, N.A.*, 147 F. Supp. 3d 937, 943 (N.D. Cal.  
8 2015); *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990).

9           Fraser’s claim for breach of the implied covenant of good faith and fair dealing parrots  
10 his breach of contract claim and seeks the same relief. The separate claim for the implied  
11 covenant is consequently **DISMISSED WITH PREJUDICE**. The allegations will be treated as part  
12 of the contract claim.

13           Second, Fraser also asserts a claim for breach of an implied-in-fact contract. A “contract  
14 implied in fact consists of obligations arising from a mutual agreement and intent to promise  
15 where the agreement and promise have not been expressed in words.” *Retired Emps. Ass’n of*  
16 *Orange Cty., Inc. v. Cty. of Orange*, 52 Cal. 4th 1171, 1178 (2011) (quotation omitted).  
17 Instead, the existence and terms are manifested by conduct; beyond that, implied-in-fact  
18 contracts have the same legal effect and basic elements as express contracts. *Dones v. Life Ins.*  
19 *Co. of N. Am.*, 55 Cal. App. 5th 665, 691 (2020); *Yari v. Producers Guild of Am., Inc.*, 161 Cal.  
20 App. 4th 172, 182 (2008).

21           Mint asserts the claim should be dismissed because there are insufficient factual  
22 allegations regarding Mint’s intent to create an implied-in-fact contract, the “very heart” of  
23 such an agreement. *See Div. of Labor Law Enf’t v. Transpacific Transp. Co.*, 69 Cal. App. 3d  
24 268, 275 (1977). Fraser, however, adequately alleges his subscription to Mint’s service and  
25 how it violated its “commitment to maintain confidentiality and security” as reflected in its  
26 privacy policy and terms and conditions (Compl. ¶¶ 243–44). Further, per Rule 8, Fraser  
27 properly asserts this theory of recovery in the alternative and alleges that it would apply “[t]o  
28 the extent that Mint’s Privacy Policy and Terms and Conditions did not form express

contracts” (*id.* ¶ 242). *Cf. Lance Camper Mfg. Corp. v. Republic Indem. Co.*, 44 Cal. App. 4th 194, 203 (1996). This order finds the specific allegations for the implied-in-fact contract limited but, for now, may proceed.

#### 5. NEGLIGENCE (COUNTS VII–IX).

To state a claim for negligence in California, a plaintiff must establish a duty, a breach of that duty, proximate cause, and damages. *See Corales v. Bennett*, 567 F.3d 554, 572 (9th Cir. 2009). Generally, purely economic losses are not recoverable in tort. *Seely v. White Motor Co.*, 63 Cal. 2d 9, 18 (1965). Put simply, “the economic loss rule prevent[s] the law of contract and the law of tort from dissolving one into the other.” *Robinson Helicopter Co. v. Dana Corp.*, 34 Cal. 4th 979, 988 (2004) (quotation omitted).

If a plaintiff’s harms are purely economic, courts employ a six-part test to determine whether a “special relationship” existed between the parties that demonstrates that defendant owed plaintiff a duty of care such that an action in tort may be maintained. *See J’Aire Corp. v. Gregory*, 24 Cal. 3d 799, 804 (1979). The *J’Aire* test considers: (1) the extent to which the transaction was intended to affect the plaintiff; (2) the foreseeability of harm to the plaintiff; (3) the degree of certainty that the plaintiff suffered injury; (4) the closeness of the connection between the defendant’s conduct and the injury suffered; (5) the moral blame attached to the defendant’s conduct; and (6) the policy of preventing future harm. *Ibid.* “The *J’Aire* court emphasized that the foreseeability of the economic harm to the plaintiff from the defendant’s negligent conduct was the critical factor.” *N. Am. Chem. Co. v. Super Ct.*, 59 Cal. App. 4th 764, (1997). Reviewing courts, nevertheless, perform a holistic review. *See Southern California Gas Leak Cases*, 7 Cal. 5th 391, 401 (2019).

As an initial matter, Mint does not contest the third or sixth factors, which, on this procedural posture, this order will view as favoring a special relationship. We turn to the remaining factors.

First, previous SIM-hijacking decisions have split on whether the first factor supports a special relationship. *Compare Terpin v. AT&T Mobility, LLC*, 2020 WL 883221, at \*4 (C.D. Cal. Feb. 24, 2020) (Judge Otis D. Wright, II), with *Shapiro v. AT&T Mobility, LLC*, 2020 WL

4341778, at \*3 (C.D. Cal. May 18, 2020) (Judge Consuelo B. Marshall). This order finds *Shapiro* persuasive on this issue — there are no allegations that the wireless services Mint offered to Fraser were “‘intended to affect’ the plaintiff[] in any way particular to the plaintiff[], as opposed to all potential purchasers” of the service. *Ott v. Alf-Laval Agri, Inc.*, 31 Cal. App. 4th 1439, 1455 (1995). The allegations here do not support a plausible inference Fraser can satisfy the first factor.

*Second*, the complaint provides sufficient allegations that the harm to Fraser was foreseeable. The complaint avers that SIM hijacking is an increasingly common crime that can arise out of the data breach of a wireless carrier (Compl. ¶¶ 37–40, 48, 61–62). Mint’s customers were actively petitioning the company for enhanced security such that Mint’s co-founder Rizwan Kassim released a public response to their inquiries (*id.* ¶¶ 45–47). The complaint explains how Mint has a federal statutory obligation to protect the personal information of its customers, and that the FCC has promulgated rules on these issues (*id.* ¶¶ 68–80). Further, Mint’s own terms and conditions and privacy policy explicitly reference the importance of privacy and keeping data secure (*id.* ¶¶ 81–86). As noted above, Fraser alleges that he added extra security (PIN verification) to his account prior to the SIM port out, but that Mint “bypassed th[at] enhanced security” when it took away control of his account (*id.* ¶ 60). Finally, the complaint alleges how Mint’s data breach and the SIM port-out provided all the information and access criminals needed to drain Fraser’s Ledger account (*id.* ¶ 63–67). This order finds these allegations sufficient to plausibly satisfy the second *J’Aire* factor. *See Shapiro*, 2020 WL 4341778, at \*3; *Terpin*, 2020 WL 883221, at \*4; *Ross v. AT&T Mobility, LLC*, 2020 WL 9848766, at \*15 (N.D. Cal. May 14, 2020) (Judge Jon S. Tigar).

Skipping to the *fourth* factor, for the same reasons discussed in the proximate cause analysis above, the complaint plausibly alleges a sufficiently close connection between Mint’s conduct and Fraser’s injury. *See, e.g., Shapiro*, 2020 WL 4341778, at \*3.

Considering the *fifth* factor, the allegations previously discussed support this order’s conclusion that the complaint plausibly alleges Mint’s moral blame. For example, the complaint alleges that Mint bypassed or failed to implement the PIN verification Fraser put in

place to protect his account days before the SIM port-out occurred (Compl. ¶¶ 60–66). This plausibly demonstrates a level of moral blame. *See Shapiro*, 2020 WL 4341778, at \*4.

Upon a holistic review, this order finds the *J'Aire* factors support the conclusion, at this stage, that Mint had a special relationship with Fraser. Fraser adequately states claims for negligence.

#### 6. PUNITIVE DAMAGES (ALL COUNTS).

Mint next argues the complaint fails to properly allege punitive damages. Fraser generally seeks punitive damages in his prayers for relief and specifically seeks punitive damages in “Wherefore” paragraphs for all his claims except declaratory judgment of the unenforceability of Mint’s consumer agreement.

For the state-law claims, under California Civil Code Section 3294(a), a plaintiff may recover punitive damages “[i]n an action for the breach of an obligation not arising from contract, where it is proven by clear and convincing evidence that the defendant has been guilty of oppression, fraud, or malice.” To establish corporate punitive damages liability, the plaintiff must prove “the wrongful act giving rise to the exemplary damages [were] committed by an ‘officer, director, or managing agent.’” *White v. Ultramar, Inc.*, 21 Cal. 4th 563, 572 (1999) (quoting Cal. Civ. Code § 3294(b)). Punitive damages are appropriate if the defendant’s acts are reprehensible, fraudulent, or in blatant violation of law or policy. *Tomaselli v. Transamerica Ins. Co.*, 25 Cal. App. 4th 1269, 1287 (1994).

To start, as a matter of law, punitive damages are not available for Section 17200 claims and contract claims. *See Clark*, 50 Cal. 4th at 610 (Section 17200); *Applied Equip. Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal. 4th 503, 516 (1994) (contract). This order accordingly **DISMISSES WITH PREJUDICE** the individual requests for punitive damages contained in the “Wherefore” paragraphs of Counts IV–VI and X–XII. *See Whittlestone, Inc. v. Handi-Craft Co.*, 618 F.3d 970, 974–76 (9th Cir. 2010).

The only remaining state-law claims to consider, then, are Fraser’s negligence claims. The California Supreme Court has stated that “punitive damages sometimes may be assessed in unintentional tort actions under Civil Code section 3294.” *Potter v. Firestone Tire & Rubber*

Co., 6 Cal. 4th 965, 1004 (1993). However, “Negligence, even if gross or reckless, cannot justify punitive damages.” *Lee v. Bank of Am.*, 218 Cal. App. 3d 914, 920 (1990); *see also Flayac v. Humrichouse*, 855 F.2d 861 (9th Cir. 1988) (mem.).

Fraser’s factual allegations on this issue rank as conclusory and lack any factual underpinning:

MINT’s misconduct as alleged herein is malice, fraud, or oppression in that it was despicable conduct carried on by MINT with a willful and conscious disregard of the rights or safety of Plaintiff and despicable conduct that has subjected Plaintiff to cruel and unjust hardship in conscious disregard of his rights

(Compl. ¶ 209; *see also* ¶ 230). The complaint contains no factual allegations that Mint’s conduct went beyond recklessness or otherwise qualified as conscious disregard of its duty of care towards Fraser. The instant allegations are distinguishable from those in *Ross*, where the punitive damages claim survived. In *Ross*, the plaintiff alleged that AT&T’s employees had worked with the hackers who performed the SIM hijacking, and that the FCC had previously fined AT&T because its employees had accessed and sold the data of thousands of AT&T customers to third parties. 2020 WL 9848766, at \*2, \*18. Here, Fraser’s allegations regarding Mint employees’ conscious involvement in a SIM hijacking (*e.g.*, Compl. ¶ 41), rank as conclusory and need not be accepted as true. Fraser’s request for punitive damages for his state-law negligence claims are **DISMISSED**.

Turning to plaintiff’s federal claims, the analysis is similar. Generally, “absent clear direction to the contrary by Congress, the federal courts have the power to award any appropriate relief in a cognizable cause of action brought pursuant to a federal statute.” *Franklin v. Gwinnett Cnty. Pub. Schs.*, 503 U.S. 60, 70–71 (1992).

The plain language of the CFAA does not authorize punitive damages. Section 1030(g) recites, in relevant part: “Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.” Given the plain language of the statute, this order finds that the CFAA limits monetary relief to compensatory damages and does not permit

a request for punitive damages. *See, e.g., Massre v. Bibiyan*, 2014 WL 2722849, at \*3 (S.D.N.Y. June 16, 2014) (Judge Katherine P. Failla).

Turning to the Federal Communications Act, Section 206 states in relevant part, that upon a finding of liability the common carrier “shall be liable to the person or persons injured thereby for the full amount of damages sustained in consequence of any such violation of the provisions of this chapter, together with a reasonable counsel or attorney’s fee.” The Supreme Court has “held that where a statute provides recovery for ‘damages sustained,’ the recovery does not include punitive damages.” *Nat’l Comms. Ass’n, Inc. v. Am. Tel. & Tel. Co.*, 1998 WL 118174, at \*31–33 (S.D.N.Y. Mar. 16, 1998) (Judge Loretta A. Preska) (citing *Local 20, Teamsters, Chauffeurs & Helpers Union v. Morton*, 377 U.S. 252, 260–61 (1964)). In light of the plain language of the statute, this order finds the Federal Communications Act does not permit a punitive damages remedy. *See also, e.g., Cahnmann v. Sprint Corp.*, 133 F.3d 484, 491 (7th Cir. 1998). Consequently, this order **DISMISSES WITH PREJUDICE** the individual requests for punitive damages specified in the “Wherefore” paragraphs for Counts II and III.

### CONCLUSION

For the foregoing reasons, the motion is **GRANTED IN PART** and **DENIED IN PART**. Plaintiff’s specific requests for punitive damages for his Section 17200 claims, contract claims, CFAA claim, and Federal Communications Act claim are **DISMISSED WITH PREJUDICE**. His specific request for remedies beyond restitution and injunctive relief as to his Section 17200 claims are also **DISMISSED WITH PREJUDICE**. His request for punitive damages as to his negligence claims are **DISMISSED**.

Further, plaintiff’s separate implied covenant of good faith and fair dealing claim is **DISMISSED WITH PREJUDICE**. Those allegations shall be treated as part of the breach of contract claim. Plaintiff’s CFAA claim and Section 17200 claims are **DISMISSED**. Defendant’s motion is otherwise **DENIED**.

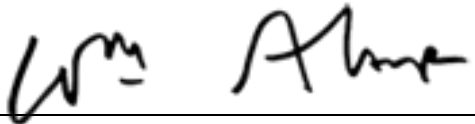
Plaintiff may move for leave to amend as to the claims dismissed without prejudice. Any such motion shall be due by **MAY 11 AT NOON**. Any such motion must include as an exhibit a redlined version of the proposed amendment that clearly identifies all changes from the current



1 complaint. This order highlighted certain deficiencies in the complaint, but it will not  
2 necessarily be enough to add sentences parroting each missing item identified herein. If  
3 plaintiff moves for leave to file another amended complaint, he should be sure to plead his best  
4 case and account for all criticisms, including those not reached by this order.

5 **IT IS SO ORDERED.**

6  
7 Dated: April 27, 2022.

8  
9 

10 WILLIAM ALSUP  
11 UNITED STATES DISTRICT JUDGE  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28